IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/791,321
Confirmation Number:	1828
Filing Date:	March 2, 2004
Applicant:	Christopher N. KLINE
Title:	SYSTEM, METHOD AND PROGRAM PRODUCT FOR MANAGING PRIVILEGE LEVELS IN A COMPUTER SYSTEM
Examiner:	Amare F. TABOR
Group Art Unit:	2139
Attorney Docket No.:	END920030127US1 (1397-12U)

Mail Stop Appeal Brief - Patents
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed August 29, 2008, and in response to the Final Office Action dated July 9, 2008, wherein Appellant appeals from the Examiner's rejection of Claims 1-14, 16 and 17.

TABLE OF CONTENTS

I. Real Party in Interest

The real party in interest is International Business Machines, which is the assignee of the subject application by virtue of assignment recorded on Reel/Frame 014517/0637 on April 14, 2004.

II. Related Appeals and Interferences

None.

III. Status of Claims

Claims 1-14, 16 and 17 are pending in this Application. Claim 15 has previously been cancelled without prejudice and without disclaimer of subject matter. Claims 1-14, 16 and 17 have been finally rejected, and it is from the final rejection of Claims 1-14, 16 and 17 that this Appeal is taken.

IV. Status of Amendments

The claims have not been amended subsequent to the imposition of the Final Office Action dated July 9, 2008.

V. Summary of Claimed Subject Matter

The present invention, as recited in independent Claims 1, 6, 11, 16 and 17 is directed toward a system and computer program products for determining that a group has been improperly assigned a privilege level higher than user level privilege, and computer program

products for managing privileges of groups, as described at least in the Summary of the Invention on pages 4-5 of the Specification.

With respect to independent Claim 1, a computer program product for determining that a group has been improperly assigned a privilege level higher than user level privilege is claimed. (See FIG. 1, privilege checking program 50; page 4, lines 1-12; and page 10, lines 24-29). The group includes a plurality of members. (See FIG. 1, list of groups and their members 40; page 8, lines 18-20). The computer program product comprises a computer readable medium having program instructions recorded thereon. (See page 4, lines 1-12; and page 13, lines 9-12). The first program instructions compare each member within the groups to a first list. (See FIG. 2(B), step 218; and page 12, lines 6-10). The first list includes names of trusted individuals. (See FIG. 1, list of trusted individuals 54; FIG. 2(A), step 100; page 8, lines 20-23; page 9, lines 27-28; and page 12, lines 9-10). The second program instructions determine whether the group includes at least one member not on the first list. (See FIG. 2(B), step 218; page 12, lines 6-13). If so, the second program instructions generate a report identifying the at least one member not on the first list and the group in which the at least one member is a member. (See FIG. 2(B), step 220; page 12, lines 10-13). The third program instructions determine whether the group has a group name on a second list. (See FIG. 2(B), step 206; page 11, lines 6-10). The second list includes group names generally used for a group with user level privilege. (See FIG. 1, list of group names presumed to be untrusted 58; FIG. 2(B), step 204; page 9, lines 2-7; page 11, lines 7-10). If so, the third program instructions generate a report indicating that the group has a group name generally used for a group having user level privilege, such that members of the group are revealed as potentially not trusted. (See FIG. 2(B), step 208; page 11, lines 15-20).

Independent Claim 6 recites a computer system for determining that a group having a plurality of members has been improperly assigned a privilege level higher than user level privilege. (See FIG. 1, computer system 10; page 4, lines 1-12; page 7, line 1 through page 9, line 12; and page 10, lines 24-29). Regarding the means-plus-function clauses of Claim 6, exemplary structure in the specification for performing the claimed functions is indicated {in brackets}. General support for the claim elements in the specification is discussed separately below. The claimed system includes a means {step 218 of privilege checking program 50 operating on computer 11} for comparing members within the group to a first list. Claim 6 further recites a means { steps 218-220 of privilege checking program 50 operating on computer 11} for determining whether the group includes at least one member not on the first list, and if so, generating a report identifying the at least one member and the group in which the at least one member is included. Claim 6 also recites a means {steps 204-206 of privilege checking program 50 operating on computer 11} for determining whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege.

Regarding the support for Claim 6 in the Specification, referring to FIG. 1, as described at least in pages 7-9 of the Specification, the claimed computer system includes computer 11 having a multiplicity of processing applications. (See FIG. 1; page 4, lines 1-12; page 9, lines 13-22). The claim recites a means for comparing members within the group to a first list. (See FIG. 2(B), step 218; and page 12, lines 6-10). The first list includes names of trusted individuals. (See FIG. 1, list of trusted individuals 54; FIG. 2(A), step 100; page 8, lines 20-23; page 9, lines 27-28; and page 12, lines 9-10). Claim 6 further recites a means for determining whether the group includes at least one member not on the first list, and if so, generating a report identifying

the at least one member and the group in which the at least one member is included. (See FIG. 2(B), steps 218-220; page 12, lines 6-13). Claim 6 also recites a means for determining whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege. (See FIG. 1, list of group names presumed to be untrusted 58, FIG. 2(B), steps 204-206; page 9, lines 2-7, page 11, lines 6-10). If so, the means generates a report indicating that the group has a group name generally used for a group with user level privilege, such that the members of the group are revealed as potentially not trusted. (See FIG. 2(B), step 208; page 11, lines 15-20).

Independent Claim 11 recites a computer program product for determining that a group having a plurality of members has been improperly assigned a privilege level higher than user level privilege. (See FIG. 1, privilege checking program 50, list of groups and their members 40; page 4, lines 1-12; page 8, lines 18-20; and page 10, lines 24-29). The computer program product comprises a computer readable medium having program instructions recorded thereon. (See page 4, lines 1-12; and page 13, lines 9-12). The first program instructions compare each member within the group to a first list. (See FIG. 2(B), step 218; and page 12, lines 6-10). The first list includes names of trusted individuals. (See FIG. 1, list of trusted individuals 54; FIG. 2(A), step 100; page 8, lines 20-23; page 9, lines 27-28; and page 12, lines 9-10). The second program instructions determine whether the group includes at least one member not on the first list, and if so, generate a report identifying the at least one member not on the first list and the group in which the at least one member is a member. (See FIG. 2(B), steps 218-220; page 12, lines 6-13). The third program instructions determine whether the group has a group name not on a second list, the second list including group names generally used for a group having a privilege level higher than user level privilege. (See FIG. 1, list of group names presumed to be

trusted 56, FIG. 2(B), step 212-214; page 8, line 23 through page 9, line 2; page 11, line 29 through page 12, line 1). If so, the third program instructions generate a report indicating that the group has a group name not generally used for a group having a privilege level higher than user level privilege, such that the members of the group are revealed as potentially not trusted. (See FIG. 2(B), step 216; page 12, lines 1-15).

Independent Claim 16 recites a computer program product for managing group privileges. (See FIG. 1, privilege checking program 50; page 4, lines 1-12; and page 9, lines 13-24). The computer program product comprises a computer readable medium having program instructions recorded thereon. (See page 4, lines 1-12; and page 13, lines 9-12). The first program instructions determine that a group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege. (See FIG. 1, list of group names presumed to be untrusted 58; FIG. 2(A), step 116; page 10, lines 12-167). Responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name generally used for a group with a privilege level no higher than user level privilege, the second program instructions compare members of the group to a list of trusted individuals. (See FIG. 1, list of trusted individuals 54; FIG. 2(A), steps 100, 104; page 8, lines 20-23; page 9, line 27 through page 10, line 3). If any member of the group does not appear on the list of trusted individuals, the second program instructions further remove the member from the group. (See FIG. 2(A), step 118; page 10, lines 16-21).

Independent Claim 17 recites a computer program product for managing privileges of groups. (See FIG. 1, privilege checking program 50, list of groups and their members 40; page 4, lines 1-12; page 8, lines 18-20; and page 10, lines 24-29). The computer program product comprises a computer readable medium having program instructions recorded thereon. (See

page 4, lines 1-12; and page 13, lines 9-12). The first program instructions determine that a group with an actual privilege level higher than user level privilege has a group name not on a list of group names generally used for a group with privilege level higher than user level privilege. (See FIG. 1, list of group names presumed to be trusted 56, FIG. 2(B), step 212-214; page 8, line 23 through page 9, line 2; page 11, line 29 through page 12, line 1). Responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name not generally used for a group with privilege level higher than user level privilege, the second program instructions compare members of the group to a list of trusted individuals. (See FIG. 1, list of trusted individuals 54; FIG. 2(A), step 100; FIG. 2(B), step 218; page 8, lines 20-23; page 9, lines 27-28; and page 12, lines 6-10). If any member of the group does not appear on the list of trusted individuals, the second program instructions lower the actual privilege level of the group. (See FIG. 2(C), step 226; page 12, lines 22-25).

VI. Grounds of Rejection to be Reviewed on Appeal

1. Claims 1, 3, 6, 8 and 11 are rejected under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter. The examiner indicates that the phrase "potentially not trusted" renders the claims indefinite.
2. Claims 1-14, 16 and 17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Applicant's Admitted Prior Art in view of United States Patent No. 7,219,234 B1, issued to Ashland et al. (hereinafter "Ashland").
3. Claims 1-14 and 16 are rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent No. 6,023,765, issued to Kuhn

(hereinafter "Kuhn") in view of United States Patent No. 7,237,119, issued to Clark et al. (hereinafter "Clark").

4. Claim 17 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Kuhn in view of European Patent No. 1112184, issued to Morris et al. (hereinafter "Morris").

VII. Argument

Claims 1, 6, 11, 16 and 17 are independent.

A. The Rejection of Claims 1, 3, 6, 8 and 11 under 35 U.S.C. § 112, second paragraph

Claims 1, 3, 6, 8 and 11 are rejected under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter. On page 5 of the Office Action, the Examiner incorrectly asserts that, with respect to Claims, 1, 3, 6, 8 and 11, the phrase "potentially not trusted" renders the claims indefinite. The Examiner provides no basis for this contention other than his conclusion of indefiniteness. Appellant disagrees with this assertion, as the meaning of the phrase "potentially not trusted" is quite clear.

It is well-known that "patent claims must be given their 'accustomed', 'ordinary', or dictionary meaning unless the available interpretation aids point to another meaning."[1] "If there is a discernable plain and ordinary meaning of the claim language, then this meaning usually defines the scope of the claims unless the patentee has explicitly disclaimed or clearly avowed this meaning in the specification or prosecution history," *Housey Pharmaceuticals, Inc. v. Astrazeneca UK Ltd.*, 366 F.3d 1348, 1352 (Fed. Cir. 2004).

1. 5A DONALD S. CHISUM, CHISUM ON PATENTS § 18.03[2][b] (2007).

Claims 1, 6 and 11 recite, in part, generating a "report indicating that the group has a group name generally used for a group with user level privilege, such that the members of the group are revealed as *potentially not trusted*," (emphasis added). Appellant contends that phrase "potentially not trusted" means that the identified members of the group may not be trusted. In other words, these members are "*suspect*". Support for this language may be found, at least at page 9, lines 14-18, a relevant portion of which is duplicated as follows:

> As described in more detail below with reference to Figures 2(A), 2(B) and 2(C), privilege checking program 50 identifies as ***suspect*** (a) groups with actual, higher privilege whose names are generally associated with untrusted, user groups, and (b) groups with actual, higher privileges whose names are not generally associated with trusted groups. (emphasis added).

The word "suspect," according to its commonly used form, means "to doubt or mistrust."[2] Additionally, the word "doubt" means "to be uncertain about something."[3] Thus, any member that is "potentially not trusted," or whose trustworthiness is doubtful, is considered suspect. As for the contention that this phrase renders the above claims indefinite, this phrase absolutely and finitely identifies a particular set of members – those members whose trust status is currently suspect.

Accordingly, independent Claims 1, 6 and 11 are directed toward definite subject matter in compliance with 35 U.S.C. § 112 and the Examiner's rejection should be reversed with respect to Claims 1, 3, 6, 8 and 11. Claims 3 and 8 depend from Claim 1 and 6, respectively, and are believed patentable at least by virtue of their dependency.

---

2. suspect. Dictionary.com. *Dictionary.com Unabridged (v 1.1)*. Random House, Inc. http://dictionary.reference.com/browse/suspect (accessed: October 14, 2008).

3. doubt. Dictionary.com. *Dictionary.com Unabridged (v 1.1)*. Random House, Inc. http://dictionary.reference.com/browse/doubt (accessed: October 14, 2008).

B. The Rejection of Claims 1-14, 16 and 17 under 35 U.S.C. § 103(a)

Claims 1-14, 16 and 17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Applicant's Admitted Prior Art (hereinafter "AAPA") in view of Ashland. Applicant disagrees with this conclusion as the Examiner has failed to cite a reference or combination of references disclosing each and every element of Applicant's Claimed Invention.

When determining the patentability of a claimed invention, the Examiner initially bears the burden of establishing a *prima facie* conclusion of obviousness. MANUAL OF PATENT EXAMINING PROCEDURE (MPEP), § 2142. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). See also *KSR International Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007)(quoting Federal Circuit statement with approval).

A conclusion that a claim would have been obvious is supported when "all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination yielded nothing more than predictable results to one of ordinary skill in the art." MPEP § 2143(A) (citing *KSR*, 127 S. Ct. at 1739).

Independent Claim 1

Regarding Claim 1, the Examiner incorrectly contends that the AAPA discloses "third program instructions to determine whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege, and if so, generate a report indicating ***that the group has a group name generally used for a group having***

user level privilege, such that members of the group are revealed as potentially not trusted," (emphasis added). Applicant disagrees with this assessment.

Specifically, the Examiner cites to page 2, lines 16-18 of the Application, which is duplicated below, along with additional excerpts of the relevant paragraph:

> With a Unix operating system, certain group names such as "staff", "users" and "nobody", are generally used for untrusted users, i.e. those with "user" privilege. Other operating systems likewise have certain group names which are generally used for "user" groups. Unix operating system and other operating systems also have certain group names which are generally used for "super user" groups such as "root" and "system", and certain group names which are generally used for "application" groups, such as "mqm" and "db2admin". (Group names will vary by application.). Occasionally, a systems administrator with "application" level privilege or "super user" privilege will change the privilege level of the "staff", "user" or "nobody" group or other such group to a higher level of privilege for a particular application. Consequently, all people in the group will get more than "user" level privilege, and some may not warrant such privilege. It was previously known for a system administrator to periodically, manually enter commands into the computer to output the group names and their privilege levels to a text file. Then, the systems administrator would review the privilege level for each group name to determine if the group names typically used for user groups (as known by the systems administrator) have higher than "user" level privilege. (Application, p. 2, lines 6-20).

In contrast to the Examiner's contention, the above excerpt does ***not*** disclose generating a report "indicating ***that the group has a group name generally used for a group having user level privilege, such that members of the group are revealed as potentially not trusted***." The only "report" generated above is a text file which merely serves to list all the group names and their associated privileges. The report does not identify ***any*** groups as being potentially untrusted, nor is such a report revealed anywhere else in the AAPA or in Ashland.

Additionally, the Examiner acknowledges that the AAPA does not disclose a first list of trusted individuals or a second list of group names. The Examiner further concedes that the AAPA does not disclose "a computer program product, recorded on a computer readable

medium, for determining that a group has been improperly assigned a privilege higher than user level privilege, the group including a plurality of members," as recited in the preamble of Claim 1. However, the Examiner incorrectly relies upon Ashland to disclose these elements.

Regarding the contention that Ashland discloses a first list of trusted individuals and a second list of group names generally used for a group with user level privilege, the Applicant disagrees with the Examiner's characterization of Ashland. The Examiner merely cites to the identification of multiple users "[see **USERID 1, USERID 2, … USERID 6** in FIG. 4]" as disclosing a list of trusted individuals. The Examiner then cites to the identification of multiple group names "[see **GROUPS – GROUP 1, GROUP 2, … GROUP N** in FIG. 4]" as disclosing a list of group names generally used for a group with user level privilege.

The USERIDs shown in FIG. 4 of Ashland only identify the actual members of specific groups. These members are not identified as "trusted individuals," nor can any assumptions be drawn from this grouping in relation to privilege levels. In fact, Ashland specifically states, in reference to FIG. 4, "It may be noted that unlike the system shown in FIG. 3, the groups of the current invention only make associations between userids. The groups ***do not*** correlate these userids with either ***privileges*** or ***access rights***." (See Ashland, col. 6, lines 63-66).

Additionally, Ashland does not teach, disclose or suggest that the GROUPs identified in FIG. 4, or anywhere else, are a listing of group names "generally used for a group with user level privilege." In fact, there is absolutely no mention in the entirety of Ashland concerning the content of the group name or that certain group names may generally be reserved for user level privileges. The actual group is clearly defined in Ashland as "a record … created to associate a particular user with the access rights that have been granted to the users of the group for referencing a particular object. The group identifies the user via the user's identification, or

'userid'. The group record further identifies the various privileges that have been assigned to the user." Thus, Ashland uses the name GROUPx as a placeholder to indicate different groupings of users, but it does not teach, disclose or suggest a listing of group names generally reserved for user level privileges.

In contrast, the computer program product of Claim 1, clearly recites the explicit use of a first list of trusted individuals and a second list of group names generally used for a group with user level privilege to determine that a group has been improperly assigned a privilege higher than user level privilege. The procedures referenced in the AAPA do not involve comparing members to a ***list of trusted individuals***, nor do they involve determining if a group with a privilege level higher than user level is on a ***list of group names*** generally used for a group with user level privilege. The procedures in the AAPA rely exclusively on the general knowledge of the system administrator. There is no mention of any type of list being referenced at all. In fact, this lack of standards is one of the problems that the AAPA specifically references as needing to be solved, as indicated by the statement, "Also, some system administrators did not know which group names were typically used for unprivileged users." (See page 2, lines 30-31). The methods discussed in the AAPA, not only fail to reveal each and every element of claim 1 as asserted in the Office Action, they are also insufficient and inferior to those claimed in the present invention as the AAPA methods yielded inconsistent and often inaccurate results.

Additionally, "statements in the preamble reciting the purpose or intended use of the claimed invention must be evaluated to determine whether the recited purpose or intended use results in a structural difference (or, in the case of process claims, manipulative difference) between the claimed invention and the prior art. If so, the recitation serves to limit the claim." MANUAL OF PATENT EXAMINING PROCEDURES § 2111.02 (8th ed. September 2007). "[C]lear

reliance on the preamble during prosecution to distinguish the claimed invention from the prior art transforms the preamble into a claim limitation because such reliance indicates use of the preamble to define, in part, the claimed invention." *Catalina Mktg. Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 808-09 (Fed. Cir. 2002).

During prosecution of the present application, Applicant clearly relied on the preamble of Claims 1, 6 and 11 to distinguish the claimed invention from the prior art. In Applicant's Response to the Office Action dated February 19, 2008, Applicant presented the argument that "determining if any of a plurality of groups may have an improper actual level of privilege" was not taught or suggested by the previously cited references. *See* Response, at 20-21. As Applicant has clearly relied on the features recited in the preamble during the course of prosecution, the features in the preamble should be considered as a claim limitation.

The Examiner has mischaracterized the Ashland reference as disclosing "a computer program, recorded [on] a computer readable medium [see FIGS. 1, 2, 4 and 5], for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members [abstract]." (See pp. 5-6 of the Office Action). However, Ashland actually teaches "a system and method ... for managing system-level privileges and for granting access rights to system resources within a data processing system." (Ashland, abstract; see also col. 6, lines 33-35. In contrast, the present invention, as recited in Claim 1, provides a method "for determining that a group has been improperly assigned a privilege level higher than user level privilege." In effect, the present invention may be viewed as a checks-and-balances system for ensuring that methods that actually assign privilege rights, such as the method disclosed by Ashland, are performing correctly.

Both the AAPA and Ashland, whether considered standing alone or in combination, fail to teach, disclose or suggest each and every element as recited in Claim 1, as required to establish a *prima facie* case of obviousness. Accordingly, the Examiner's rejection with respect to Claim 1 should be reversed.

Independent Claim 6

Independent Claim 6 also recites features similar to those discussed above in relation to Claim 1. Specifically, independent Claim 6 includes "a computer system for determining that a group has been improperly assigned a privilege level higher than user level privilege" as well as means for performing each of the functions executed by the programming instructions of Claim 1. Thus, the arguments presented above in relation to Claim 1, apply equally to independent Claim 6 and the rejection under 35 U.S.C. § 103(a) should be reversed.

Independent Claim 11

With respect to independent Claim 11, the Examiner incorrectly contends that the AAPA discloses "third program instructions to determine whether the group has a group name not on a second list, the second list including group names generally used for a group having a privilege level ***higher*** than user level privilege, and if so, generate a report indicating that the group has a group name not generally used for a group having a privilege level higher than user level privilege, such that the members of the are revealed as potentially not trusted," (emphasis added). Applicant completely disagrees with this contention and earnestly believes the Examiner has misread the AAPA.

In fact, page 2, lines 18-20 state, "Then, the systems administrator would review the privilege level for each group name to determine if the ***group names typically used for user groups*** (as known by the systems administrator) have higher than "user" level privilege." In

which case, the administrator, through personal knowledge, attempted to determine groups having an errant privilege level. However, there is absolutely no mention of determining whether a group is on a second list which explicitly lists group names generally used for a group having a privilege level ***higher*** than user level privilege.

Additionally, the Examiner further relies upon the teachings of Ashland as disclosing a first list of trusted individuals, a second list of group names generally used for a group having a privilege level ***higher*** than user level privilege, and "a computer program product, recorded on a computer readable medium, for determining that a group has been improperly assigned a privilege higher than user level privilege, the group including a plurality of members," as indicated above in relation to independent Claim 1. Thus, the arguments presented above in the discussion of Claim 1 regarding these elements, apply equally to independent Claim 11. Both the AAPA and Ashland, whether considered standing alone or in combination, fail to teach, disclose or suggest each and every element as recited in Claim 11, as required to establish a *prima facie* case of obviousness. Accordingly, the Examiner's rejection with respect to Claim 11 should be reversed.

Independent Claim 16

Regarding Claim 16, the Examiner incorrectly contends that the AAPA discloses the feature of "second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name generally used for a group with a privilege level no higher than user level privilege, to compare members of said group to a list of trusted individuals, and ***if any member of said group does not appear on said list of trusted individuals, remove said member from said group***." Removing said member from said group does not appear in the AAPA. In fact, the AAPA is silent as to ***any*** consequences resulting from

determining that a member of any group having privilege levels higher than user level is not on a list of trusted individuals. The only relevant comment at all is that "[s]uch a case would warrant further investigation." (See p.2, lines 20-21). This feature is simply not mentioned or suggested by such statement.

Also, as in the case of Claim 1, the Examiner concedes that the AAPA does not disclose an actual list of trusted individuals or a list containing group names generally reserved for groups having a privilege level no higher than that of user level privilege. The Examiner relies upon the teachings of Ashland as disclosing a first list of trusted individuals and a second list of group names generally used for a group with a privilege level no higher than user level privilege. Thus, the arguments presented above in the discussion of Claim 1 regarding these elements, apply equally to independent Claim 16.

Accordingly, as neither the AAPA nor Ashland teach, disclose or suggest every element of Claim 16, the Examiner has failed to establish a *prima facie* case of obviousness. Thus, the Examiner's rejection with respect to Claim 16 should be reversed.

Independent Claim 17

With respect to independent Claim 17, the Examiner incorrectly contends that the AAPA discloses "first program instructions to determine that a group with an actual privilege level higher than user level privilege has a group name not on a list of group names generally used for a group with privilege level ***higher*** than user level privilege," and "second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name not generally used for a group with privilege level higher than user level privilege, to compare members of said group to a list of trusted individuals, and ***if any***

member of said group does not appear on said list of trusted individuals, lower the actual privilege level of said group."

As discussed above in relation to independent Claim 11, there is absolutely no mention in either the AAPA or Ashland of determining whether a group with an actual privilege level higher than user level privilege has a group name not on a list which explicitly lists group names generally used for a group having a privilege level ***higher*** than user level privilege. The only discussion of generally used, or reserved, group names in the AAPA states, "Then, the systems administrator would review the privilege level for each group name to determine if the ***group names typically used for user groups*** (as known by the systems administrator) have higher than "user" level privilege." (See p.2, lines 18-20). No review of group names reserved for users having a privilege level ***higher*** than user level is taught, disclosed or suggested.

Additionally, the feature "***if any member of said group does not appear on said list of trusted individuals, lower the actual privilege level of said group,***" also does not appear in the AAPA, as contended by the Examiner. As mentioned above in relation to Claim 16, the AAPA is silent as to ***any*** consequences resulting from determining that a member of any group having privilege levels higher than user level is not on a list of trusted individuals. The only relevant comment at all is that "[s]uch a case would warrant further investigation." (See p.2, lines 20-21). The claimed feature is not even mentioned, thus it is not taught, disclosed or suggested by such statement.

Accordingly, as neither the AAPA nor Ashland teach, disclose or suggest every element of Claim 17, the Examiner has failed to establish a *prima facie* case of obviousness. Thus, the Examiner's rejection with respect to Claim 17 should also be reversed.

Dependent Claims 2-5, 7-10 and 12-14

Dependent Claims 2-5, 7-10 and 12-14 depend from one or another of independent Claims 1, 6, and 11 and are believed patentable at least by virtue of their dependency.

C. The Rejection of Claims 1-14 and 16 under 35 U.S.C. § 103(a)

Claims 1-14 and 16 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Kuhn in view of Clark.

Independent Claim 1

Regarding Claim 1, the Examiner incorrectly contends that Kuhn discloses "[a] computer program product, recorded on a computer readable medium, for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members," as recited in the preamble.

As previously established, the Applicant has clearly relied upon the preamble of Claims 1, 6 and 11 to distinguish the claimed invention from the prior art; therefore, the preamble should be interpreted as a claim limitation. Applicant respectfully disagrees with the Examiner's characterization of Kuhn as disclosing "[a] computer program product, recorded on a computer readable medium, for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members." Kuhn discloses a method for "controlling access to computer systems" through the implementation of role based access control. (See Kuhn, col. 4, lines 25-28; col. 5, lines 9-14). Thus, Kuhn discloses a method for determining whether a user has access to certain computer resources based on assigned privilege levels. Kuhn does not disclose a method of validating whether the privilege levels assigned are correct.

Additionally, the Examiner contends that Equations (1) and (4) presented in Kuhn are equivalent to the claimed feature of "second program instructions to determine whether the group includes at least one member not on the first list." Equation (1), according to the direct interpretation of Kuhn, means, "in effect, that human users are authorized to execute privileges assigned to a role only if they belong to the class of subjects authorized for that role." Equation (4), also according to Kuhn, "refers to privilege authorization: a subject can execute a privilege only if the privilege is authorized for a role in which the subject is currently active." Applicant asserts that Equations (1) and (4) simply do not equate to determining "whether the group includes at least one member ***not*** on the first list." It appears that the equations referenced in Kuhn do the exact opposite of the recited feature of Claim 1. For the method of Kuhn, i.e., determining whether a user has the authority to access a resource, the process must determine that the user ***is authorized*** to have access. However, Claim 1 is trying to determine that a member of the group ***is not authorized*** to have access, i.e., a user is not trusted.

The Examiner further contends that Equations (2) and (3) of Kuhn discloses "third program instructions to determine whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege." According to Kuhn, "Equation (2) refers to role assignment: a subject can execute a privilege only if the subject has been selected or been assigned an active role," and "Equation (3) refers to role authorization: a subject's active role must be authorized for the subject." Again, Equations (2) and (3) appear to define rules for allowing a particular user, i.e., a "subject", to have access to certain resources of a computer system. These equations do not teach, disclose, or suggest determining "whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege." In particular, Kuhn is silent

regarding comparing the group name to a second list, and the actual privilege level, i.e., "user level," of the group names included on the list.

Additionally, the Examiner concedes that Kuhn does not disclose, responsive to determining that the group has a group name on a second list, generating "a report indicating that the group has a group name generally used for a group having user level privilege, such that members of the group are revealed as potentially not trusted." The Examiner incorrectly relies upon Clark to disclose this feature. However, Clark discloses a computer application consisting of a set of templates for which a system administrator can assign privilege levels to a plurality of users. (See FIGS. 3-5; col. 3, lines 37-53). Clark does ***not*** disclose generating a report that reveals members of the group as being potentially untrusted in response to determining that the group has a group name generally used for a group having user level privilege.

Neither Kuhn nor Clark, whether considered standing alone or in combination, teach, disclose or suggest each and every element as recited in Claim 1, as required to establish a *prima facie* case of obviousness. Accordingly, the Examiner had failed to meet his burden of proof and the rejection with respect to Claim 1 should be reversed.

Independent Claim 6

Independent Claim 6 also recites features similar to those discussed above in relation to Claim 1. Specifically, independent Claim 6 includes "a computer system for determining that a group has been improperly assigned a privilege level higher than user level privilege" as well as means for performing each of the functions executed by the programming instructions of Claim 1. Thus, the arguments presented above in relation to Claim 1, apply equally to independent Claim 6 and the rejection under 35 U.S.C. § 103(a) should be reversed.

Independent Claim 11

With respect to independent Claim 11, as with Claim 1 above, the Examiner incorrectly contends that Kuhn discloses "[a] computer program product, recorded on a computer readable medium, for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members," and "second program instructions to determine whether the group includes at least one member not on the first list." Additionally, the Examiner relies upon Clark to disclose the feature where responsive to determining that the group has a group name on a second list, the third program instructions "generate a report indicating that the group has a group name generally used for a group having user level privilege, such that members of the group are revealed as potentially not trusted." Thus, the arguments presented above concerning these features in connection with Claim 1 apply equally to independent Claim 11.

Additionally, the Examiner contends that Kuhn discloses the feature of "third program instructions to determine whether the group has a group name not on a second list, the second list including group names generally used for a group having a privilege level higher than user level privilege." The Examiner again cites Equations (2) and (3) of Kuhn in support of this contention. However, these equations do not teach, disclose, or suggest determining "whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege." Nor is this feature taught, disclosed or suggested anywhere else in the entirety of the Kuhn reference. In particular, Kuhn is silent regarding comparing the group name to a second list, and the actual privilege level, i.e., "user level," of the group names included on the list.

As both Kuhn and Clark, whether considered standing alone or in combination, fail to teach, disclose or suggest each and every element as recited in Claim 11, as required to establish a *prima facie* case of obviousness. Accordingly, the Examiner's rejection with respect to Claim 11 should be reversed.

Independent Claim 16

Regarding Claim 16, the Examiner incorrectly contends that Kuhn discloses the features of "first program instructions to determine that a group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege" and "second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name generally used for a group with a privilege level no higher than user level privilege, to compare members of said group to a list of trusted individuals." These features have been discussed above in relation to Claims 1 and 11, and the arguments presented above apply equally to independent Claim 16.

The Examiner relies upon Clark as disclosing the feature where "if any member of said group does not appear on said list of trusted individuals, remove said member from said group." In support of this position, the Examiner shows that templates within the disclosed administrative application allow an administrator to delete a user from having access to a specific application. (See **Del Row** in FIGS. 4 and 7; **Level 140** in FIG. 4, and col. 3, line 46 to col. 4, line 23). However, Clark only discloses the ability to remove a member from group. It does not disclose removing the member from the group in response to determining that the member of a group having privilege levels higher than user level is not on a list of trusted individuals. In fact, Clark does not reveal that deleting a member from authorization is in any way responsive to any deterministic event at all. Neither Kuhn nor Clark, whether considered alone or in combination,

teach, disclose or suggest every element of independent Claim 16 and the rejection should be reversed.

Dependent Claims 2-5, 7-10, and 12-14

Dependent Claims 2-5, 7-10, and 12-14 depend from one of independent Claims 1, 6, and 11 and are believed patentable at least by virtue of their dependency.

D. The Rejection of Claim 17 under 35 U.S.C. § 103(a)

Claim 17 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Kuhn in view of Morris. The Examiner incorrectly contends that Kuhn discloses the features of "first program instructions to determine that a group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege" and "second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name not generally used for a group with privilege level higher than user level privilege, to compare members of said group to a list of trusted individuals." These features have been discussed in Section C above in relation to Claims 1, and the arguments presented above apply equally to independent Claim 17.

The Examiner relies upon Morris to disclose the feature where "if any member of said group does not appear on said list of trusted individuals, lower the actual privilege level of said group." In support of this position, the Examiner shows that templates within the disclosed administrative application allow an administrator to delete a user from having access to a specific application. (See **Del Row** in FIGS. 4 and 7; **Level 140** in FIG. 4, and col. 3, line 46 to col. 4, line 23). However, Morris discloses demoting a privilege level based on a comparison of a current privilege level state to a previous level state. It does not disclose lowering the actual

privilege level of an entire group based on a determination that a single member of the group does not appear on a separate list of trusted individuals. Neither Kuhn nor Morris, whether considered alone or in combination, teach, disclose or suggest every element of independent Claim 17 and the rejection should be reversed.

VIII. Conclusion

For the reasons provided above as well as provided in the record, the claim rejections are believed to be improper and a result of clear error by the Examiner. Accordingly, pending Claims 1-14, 16 and 17 are believed to be in condition for allowance, and a reversal of the Examiner's rejections is respectfully requested.

The Commissioner is hereby authorized to credit overpayments or charge payment of any additional fees associated with this communication to Deposit Account No. 090457.

Respectfully submitted,

Date: October 28, 2008

By: /Alan M. Weisberg/

Alan M. Weisberg
Reg. No.: 43,982
Attorney for Applicants
Christopher & Weisberg, P.A.
200 East Las Olas Boulevard, Suite 2040
Fort Lauderdale, Florida 33301
Customer No. 68786
Tel: (954) 828-1488
Fax: (954) 828-9122
email: ptomail@cwiplaw.com

119888

APPENDIX A: CLAIMS ON APPEAL

1. A computer program product for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members, said computer program product comprising:

a computer readable medium;

first program instructions to compare each member within the groups to a first list, the first list including names of trusted individuals;

second program instructions to determine whether the group includes at least one member not on the first list, and if so, generate a report identifying said at least one member not on the first list and the group in which said at least one member is a member; and

third program instructions to determine whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege, and if so, generate a report indicating that the group has a group name generally used for a group having user level privilege, such that members of the group are revealed as potentially not trusted; and

said first, second and third program instructions are recorded on said medium.

2. A computer program product as set forth in claim 1 wherein there are a plurality of applications or application instances, and a same group can be assigned different privilege levels for involvement with different applications or application instances; and said third program instructions makes its determination separately for each application or application instance.

3. A computer program product as set forth in claim 1, further comprising:

fourth program instructions to determine whether the group has a group name not included on a third list, the third list including group names generally used for a group-having a privilege level higher than user level privilege, and if so, generate a report indicating that the group has a group name not on the third list, such that members of the group are revealed as potentially not trusted;

wherein said fourth program instructions are recorded on said medium.

4. A computer program product as set forth in claim 1, wherein said second program instructions determine whether the group includes at least one members not on the first list, and if not, generate a report indicating that the group has all its members on the first list.

5. A computer program product as set forth in claim 1, further comprising fourth program instructions, responsive to determining that the group has a group name on the second list, to determine whether each members of the group is on the first list; and wherein

said fourth program instructions are recorded on said medium.

6. A computer system for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members, said computer system comprising:

means for comparing members within the group to a first list, the first list including names of trusted individuals;

means for determining whether the group includes at least one member not on the first list, and if so, generating a report identifying the at least one member and the group in which the at least one member is included; and

means for determining whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege, and if so, generating a report indicating that the group has a group name generally used for a group with user level privilege, such that the members of the group are revealed as potentially not trusted.

7. A computer system as set forth in claim 6 wherein there are a plurality of applications or application instances, and a same group can be assigned different privilege levels for involvement with different applications or application instances; and said means for determining whether the group has a group name generally used for a group with user level privilege makes its determination separately for each application or application instance.

8. A computer system as set forth in claim 6, further comprising:

means for determining whether the group has a group name not on a third list, the third list including group names generally used for a group having a privilege level higher than user level privilege, and if so, generating a report indicating that the group has a group name not generally used for a group with the higher level privilege, such that the members of the group are revealed as potentially not trusted.

9. A computer system as set forth in claim 6, wherein said means for determining whether the group includes at least one member not on the first list determines that the group has

all of its members on the list of trusted individuals, said means generates a report indicating that the group has all its members on the first list.

10. A computer system as set forth in claim 6, wherein responsive to determining that the group has a group name generally used for a group with user level privilege, further comprises means for determining whether the members of the group are on the first list.

11. A computer program product for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members, said computer program product comprising:

a computer readable medium;

first program instructions to compare each members within the group to a first list, the first list including names of trusted individuals;

second program instructions to determine whether the group includes at least one member not on the first list, and if so, generate a report identifying said at least one member not on the first list and the group in which said at least one member is a member; and

third program instructions to determine whether the group has a group name not on a second list, the second list including group names generally used for a group having a privilege level higher than user level privilege, and if so, generate a report indicating that the group has a group name not generally used for a group having a privilege level higher than user level privilege, such that the members of the are revealed as potentially not trusted;

said first, second and third program instructions are recorded on said medium.

12. A computer program product as set forth in claim 11 wherein there are a plurality of applications or application instances, and a same group can be assigned different privilege levels for involvement with different applications or application instances; and said third program instructions makes its determination separately for each application or application instance.

13. A computer program product as set forth in claim 11 wherein said second program instructions determine whether the group has at least one member not on the first list, and if not, generate a report indicating that the group has all its members on the first list.

14. A computer program product as set forth in claim 11 further comprising fourth program instructions, responsive to determining that the group has a group name on the second list, to determine whether each member of is on the first list; and wherein

said fourth program instructions are recorded on said medium.

15. (Cancelled)

16. A computer program product for managing privileges of groups, said computer program product comprising:

a computer readable medium;

first program instructions to determine that a group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege; and

second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name generally used for a group with a privilege level no higher than user level privilege, to compare members of said group to a list of trusted individuals, and if any member of said group does not appear on said list of trusted individuals, remove said member from said group; and wherein

said first and second program instructions are recorded on said medium.

17. A computer program product for managing privileges of groups, said computer program product comprising:

a computer readable medium;

first program instructions to determine that a group with an actual privilege level higher than user level privilege has a group name not on a list of group names generally used for a group with privilege level higher than user level privilege; and

second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name not generally used for a group with privilege level higher than user level privilege, to compare members of said group to a list of trusted individuals, and if any member of said group does not appear on said list of trusted individuals, lower the actual privilege level of said group; and

said first and second program instructions are recorded on said medium.

APPENDIX B: EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

APPENDIX C: RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.